A visible factor for analytic rank one

Amod Agashe [*]

October 29, 2008

Abstract

Let E be an optimal elliptic curve of conductor N, such that the L-function of E vanishes to order one at $s = 1$. Let K be a quadratic imaginary field in which all the primes dividing N split and such that the L-function of E over K also vanishes to order one at $s = 1$. In view of the Gross-Zagier theorem, the second part of the Birch and Swinnerton-Dyer conjecture says that the index in $E(K)$ of the subgroup generated by the Heegner point is equal to the product of the Manin constant of E, the Tamagawa numbers of E, and the square root of the order of the Shafarevich-Tate group of E (over K). We extract an integer factor from the index mentioned above and relate this factor to certain congruences of the newform associated to E with eigenforms of analytic rank bigger than one. We use the theory of visibility to show that, under certain hypotheses (which includes the first part of the Birch and Swinnerton-Dyer conjecture on rank), if an odd prime q divides this factor, then q divides the order of the Shafarevich-Tate group or the order of an arithmetic component group of E, as predicted by the second part of the Birch and Swinnerton-Dyer conjecture.

1 Introduction and results

Let N be a positive integer. Let $X = X_0(N)$ denote the modular curve over $\mathbf{Q}$ associated to $\Gamma_0(N)$, and let $J = J_0(N)$ denote the Jacobian of X, which is an abelian variety over $\mathbf{Q}$. Let $\mathbf{T}$ denote the Hecke algebra, which is the subring of endomorphisms of $J_0(N)$ generated by the Hecke operators (usually denoted T_ℓ for $\ell \nmid N$ and U_p for $p \mid N$). If g is an eigenform of weight 2 on $\Gamma_0(N)$, then let $I_g = \mathrm{Ann}_{\mathbf{T}} g$ and let A_g denote the quotient abelian

variety $J/I_g J$, which is defined over $\mathbf{Q}$. Also, if g is an eigenform of weight 2 on $\Gamma_0(N)$, then the order of vanishing of the L-function $L(g, s)$ at $s = 1$ is called the *analytic rank of g*. Let f be a newform of weight 2 on $\Gamma_0(N)$ whose analytic rank is one and which has integer Fourier coefficients. Then $E = A_f$ is an elliptic curve whose L-function vanishes to order one at $s = 1$. We denote the quotient map $J \to J/I_f = E$ by π.

Let K be a quadratic imaginary field of discriminant not equal to -3 or -4, and such that all primes dividing N split in K and such that the L-function of E over K vanishes to order one at $s = 1$. Choose an ideal $\mathcal{N}$ of the ring of integers $\mathcal{O}_K$ of K such that $\mathcal{O}_K/\mathcal{N} \cong \mathbf{Z}/N\mathbf{Z}$. Then the complex tori $\mathbf{C}/\mathcal{O}_K$ and $\mathbf{C}/\mathcal{N}^{-1}$ define elliptic curves related by a cyclic N-isogeny, hence a complex valued point x of $X_0(N)$. This point, called a Heegner point, is defined over the Hilbert class field H of K. Let $P \in J(K)$ be the class of the divisor $\sum_{\sigma \in \mathrm{Gal}(H/K)} ((x) - (\infty))^\sigma$.

By [GZ86, p.311–313], the index in $E(K)$ of the subgroup generated by $\pi(P)$ is finite; note that this subgroup is just $\pi(\mathbf{T}P)$. Also, the order of $\mathrm{III}(E/K)$ is finite, by work of Kolyvagin (see, e.g., [Gro91, Thm 1.3]). By [GZ86, §V.2:(2.2)], the second part of the Birch and Swinnerton-Dyer conjecture becomes:

Conjecture 1.1 (Birch and Swinnerton-Dyer, Gross-Zagier)**.**

$$|E(K)/\pi(\mathbf{T}P)| \stackrel{?}{=} c_E \cdot \prod_{p|N} c_p(E) \cdot \sqrt{|\mathrm{III}(E/K)|} \, , \tag{1}$$

where c_E is the Manin constant of E (conjectured to be one), and $c_p(E)$ is the Tamagawa number of E at the prime p (i.e., the order of the arithmetic component group of E at the prime p).

The theory of Euler systems can be used to show that the actual value of the order of $\mathrm{III}(E/K)$ divides the order predicted by the conjectural formula (1) (equivalently, that the right side of (1) divides the left side), under certain hypotheses, and staying away from certain primes (see [Kol90, Theorem A], and also [Gro91, Thm 1.3]). Our goal is to try to prove results towards divisibility in the opposite direction, i.e., that the left side of (1) divides the right side. In particular, we shall extract an integer factor of the left side of (1) which we will relate to congruences of f with eigenforms of analytic rank bigger than one, and these congruences will in turn be related to the right side of (1) using the theory of visibility, under certain hypotheses.

Let T be a non-empty set of Galois conjugacy classes of newforms of level dividing N and having analytic rank more than one. Let S_T denote

the subspace of $S_2(\Gamma_0(N), \mathbf{C})$ spanned by the forms $g(dz)$, where g runs over elements in the Galois conjugacy classes in T, and d ranges over the divisors of N/N_g, where N_g denote the "true level" of g. Let I_T denote the annihilator of S_T under the action of $\mathbf{T}$. Let J' denote the quotient abelian variety $J/(I_f \cap I_T)J$. The quotient map $\pi : J \to J/I_f J$ factors through $J' = J/(I_f \cap I_T)J$. Let π' denote the map $J' \to E$ and π'' the map $J \to J'$ in this factorization. Let B' denote the kernel of π'. Thus we have the following diagram:

$$
\begin{array}{ccccccccc}
 & & & & J & & & & \\
 & & & \pi'' \downarrow & & \searrow \pi & & & \\
0 & \longrightarrow & B' & \longrightarrow & J' & \xrightarrow{\ \pi'\ } & E & \longrightarrow & 0
\end{array}
$$

Note that J' and B' depend on the choice of the set T; we have suppressed the dependency in the notation for simplicity (for certain interesting choices of T, see Section 2). Let E' denote the image of $E^\vee \subseteq J$ in J' under the quotient map $\pi'' : J \to J'$ and let $\pi''(\mathbf{T}P)_f$ denote the free part of $\pi''(\mathbf{T}P)$.

Lemma 1.2. *We have $\pi''(\mathbf{T}P)_f \subseteq E'(K)$ with finite index, and*

$$
|E(K)/\pi(\mathbf{T}P)| \tag{2}
$$

$$
= \left| \frac{J'(K)}{B'(K) + E'(K)} \right| \cdot \left| \ker\!\big(H^1(K, B') \to H^1(K, J')\big) \right| \cdot \frac{\left| \frac{B'(K) + E'(K)}{B'(K) + \pi''(\mathbf{T}P)_f} \right|}{\left| \frac{B'(K) + \pi''(\mathbf{T}P)}{B'(K) + \pi''(\mathbf{T}P)_f} \right|} \ .
$$

Proof. By [Aga08, Prop. 1.6], we have

$$
|E(K)/\pi(\mathbf{T}P)| = \left| \frac{J'(K)}{B'(K) + \pi''(\mathbf{T}P)} \right| \cdot \left| \ker\!\big(H^1(K, B') \to H^1(K, J')\big) \right|. \tag{3}
$$

If h is an eigenform of weight 2 on $\Gamma_0(N)$, then $\mathbf{T}P \cap A_h^\vee(K)$ is infinite if and only if h has analytic rank one (this follows by [GZ86, Thm 6.3] if h has analytic rank bigger than one, and the fact that $A_h^\vee(K)$ is finite if h has analytic rank zero, by [KL89]). The composite $E^\vee \xrightarrow{\pi''} E' \xrightarrow{\pi'} E$ is an isogeny, and so J' is isogenous to $E' \oplus B'$. Now B' is isogenous to a product of $A_g^\vee$'s (with multiplicities) where g runs over representatives of conjugacy classes of eigenforms in T; all these eigenforms have analytic rank greater than one. Thus from the discussion above, we see that the free part of $E'(K)$ contains $\pi''(\mathbf{T}P)_f$. The lemma now follows from equation (3). We remark that the transition from equation (3) to equation (2) is analogous to the situation in the rank one case (cf. Theorem 3.1 of [Aga07] and its proof), where the idea is due to L. Merel. $\square$

3

The reason for factoring the quantity $|E(K)/\pi(\mathbf{T}P)|$, which is the left side of the Birch and Swinnerton-Dyer conjectural formula (1), as above in equation (2) is that we can say something about the factor

$$\left|\frac{J'(K)}{B'(K)+E'(K)}\right| \cdot \left|\ker\bigl(H^1(K,B')\to H^1(K,J')\bigr)\right|$$

in this factorization:

Proposition 1.3. *Suppose q is a prime that divides the product*

$$\left|\frac{J'(K)}{B'(K)+E'(K)}\right| \cdot \left|\ker\bigl(H^1(K,B')\to H^1(K,J')\bigr)\right|.$$

Then q divides the order of $B'\cap E'$, and there is an eigenform g in S_T such that f is congruent to g modulo a prime ideal $\mathfrak{q}$ over q in the ring of integers of the number field generated by the Fourier coefficients of f and g.

We will prove this Proposition in Section 3. If G is a finite abelian group and r is a prime, then let $|G|_r$ denote the order of the r-primary component of G (equivalently, $|G|_r$ is the highest power of r that divides the order of G). If q is a prime that does not divide the order of the torsion subgroup of $\pi''(\mathbf{T}P)$, then in view of equation (2), the Birch and Swinnerton-Dyer conjectural formula (1) says:

$$\left|c_{A_f} \cdot \prod_{p|N} c_p(E)\right|_q \cdot \sqrt{|\text{Ш}(E/K)|_q} \tag{4}$$

$$\stackrel{?}{=} \left|\frac{J'(K)}{B'(K)+E'(K)}\right|_q \cdot \left|\ker\bigl(H^1(K,B')\to H^1(K,J')\bigr)\right|_q \cdot \left|\frac{B'(K)+E'(K)}{B'(K)+\pi''(\mathbf{T}P)_f}\right|_q.$$

In particular, the conjecture predicts that the product

$$\left|\frac{J'(K)}{B'(K)+E'(K)}\right|_q \cdot \left|\ker\bigl(H^1(K,B')\to H^1(K,J')\bigr)\right|_q$$

divides $c_E \cdot \prod_{p|N} c_p(E) \cdot \sqrt{|\text{Ш}(E/K)|}$.

Using Proposition 1.3 and the theory of visibility, we can show the following result towards this predicted divisibility:

Theorem 1.4. *Let q be a prime that divides the product*

$$\left|\frac{J'(K)}{B'(K)+E'(K)}\right| \cdot \left|\ker\bigl(H^1(K,B')\to H^1(K,J')\bigr)\right|.$$

4

Suppose that $q \nmid 2N$ and that $E[q]$ is an irreducible representation of the absolute Galois group of K. Assume that the first part of the Birch and Swinnerton-Dyer conjecture holds for all quotients of $J_0(N)$ associated to eigenforms of analytic rank greater than one. Suppose that for all primes $p \mid N$, $p \not\equiv -w_p \pmod{q}$, where w_p is the sign of the Atkin-Lehner involution W_p acting on f. We have two possibilities:

Case (i) For all primes $p \mid N$, f is not congruent to a newform g of level dividing N/p (for Fourier coefficients of index coprime to Nq) modulo a prime ideal over q in the ring of integers of the number generated by the coefficients of f and g:

In this case, suppose that for all primes p such that $p^2 \mid N$, we have $p \not\equiv -1 \pmod{q}$.

Then q divides $|\text{III}(E)|$.

Case (ii) For some prime p dividing N, f is congruent to a newform g of level dividing N/p (for Fourier coefficients of index coprime to Nq) modulo a prime ideal $\mathfrak{q}$ over q in the ring of integers of the number generated by the coefficients of f and g:

In this case, suppose that there a triple p, g, and $\mathfrak{q}$ as above such that $p^2 \nmid N$, $w_p = -1$, and $A_g[\mathfrak{q}]$ irreducible as a representation of the absolute Galois group of $\mathbf{Q}$.

Then q divides $\prod_{p \mid N} c_p(E)$.

Proof. By Proposition 1.3, there is an eigenform g on $\Gamma_0(N)$ having analytic rank greater than one such that f is congruent to g modulo a prime ideal $\mathfrak{q}$ over q in the ring of integers $\mathcal{O}$ of the number field generated by the Fourier coefficients of f and g.

Case (i) now follows from Theorem 6.1 of [DSW03], as we now indicate (for details of some of the definitions below, see [DSW03]). Let $T_\mathfrak{q}$ denote the $\mathfrak{q}$-adic Tate module of $E^\vee = E$. Let $L_\mathfrak{q}$ denote the quotient field of $\mathcal{O}_\mathfrak{q}$, let $V_\mathfrak{q} = T_\mathfrak{q} \otimes_{\mathcal{O}_\mathfrak{q}} L_\mathfrak{q}$, and let $A_\mathfrak{q}$ denote $V_\mathfrak{q}/T_\mathfrak{q}$. We denote the corresponding objects for $A_g^\vee$ by $T'_\mathfrak{q}$, $V'_\mathfrak{q}$, and $A'_\mathfrak{q}$. Let r denote the dimension of $H^1_f(K, V'_\mathfrak{q})$ over $L_\mathfrak{q}$. Then r is at least the analytic rank of g (since we are assuming the first part of the Birch and Swinnerton-Dyer conjecture for $A_g^\vee$), i.e., at least 2. Theorem 6.1 of loc. cit. (which is stated over $\mathbf{Q}$, but works over K as well) tells us that the $\mathfrak{q}$-torsion subgroup of the Selmer group $H^1_f(K, A_\mathfrak{q})$ of $E^\vee$ has $\mathcal{O}_\mathfrak{q}/\mathfrak{q}$-rank at least r. Since the abelian group $E^\vee(K)$ has rank one, the image of $H^1_f(K, V_\mathfrak{q})$ in the $\mathfrak{q}$-torsion subgroup of $H^1_f(K, A_\mathfrak{q})$ has $\mathcal{O}_\mathfrak{q}/\mathfrak{q}$-rank at most one. This shows that $|\text{III}(E^\vee/K)|$ is divisible by q^{r-1}, in particular by $q^{2-1} = q$ (since $r \geq 2$). By the perfectness of the Cassels-Tate pairing, we see that q divides the order of $\text{III}(E/K)$ as well. This proves

Case (i). Case (ii) follows from [Aga07, Prop. 6.3]. □

Corollary 1.5. *Let q be a prime that divides the product*

$$\left|\frac{J'(K)}{B'(K) + E'(K)}\right| \cdot \left|\ker\left(H^1(K, B') \to H^1(K, J')\right)\right|.$$

Suppose that N is prime, $q \nmid N(N+1)$, and $E[q]$ is an irreducible representation of the absolute Galois group of K. Assume that the first part of the Birch and Swinnerton-Dyer conjecture holds for all quotients of $J_0(N)$ associated to eigenforms of analytic rank greater than one. Then q divides $|\text{Ш}(E)|$.

Proof. Since $w_N = 1$, we have $N \not\equiv -1 \pmod q$ by hypothesis. Also, since the level is prime, there are no newforms of lower level. The corollary now follows from Theorem 1.4. □

We remark that N. Dummigan has informed us that the hypothesis that for all primes p dividing N, $p \not\equiv -w_p \bmod q$ can be eliminated from [DSW03, Thm. 6.1], and hence from Theorem 1.4; if this is the case, then the hypothesis that $q \nmid (N+1)$ can be eliminated from the corollary above.

In view of our discussion just preceding Theorem 1.4, the theorem and corollary above are partial results towards the second part of the Birch and Swinnerton-Dyer conjecture in the analytic rank one case, and provide theoretical evidence supporting the conjecture. Also, under certain hypotheses (the most serious of which is the first part of the Birch and Swinnerton-Dyer conjecture), we have shown that if a prime q divides a certain factor of the left side of the Birch and Swinnerton-Dyer conjectural formula (1), then q divides the right side the formula (which includes $\sqrt{|\text{Ш}(E)|}$ as a factor). Thus our result is a step in trying to prove that the left side of the Birch and Swinnerton-Dyer conjectural formula (1) divides the right side. As mentioned earlier, the theory of Euler systems gives results in the opposite direction, viz., that the right side of the Birch and Swinnerton-Dyer conjectural formula (1) divides the left side (under certain hypotheses). Thus our result fits well in the ultimate goal of trying to prove the second part of the Birch and Swinnerton-Dyer conjecture in the analytic rank one case. Note that the theory of Euler systems can also be used to construct non-trivial elements of the Shafarevich-Tate group (e.g., see [McC91]).

In Section 2 we make some further remarks about our main result and in Section 3, we give the proof of Proposition 1.3.

2   Some further remarks

Note that the product

$$\left| \frac{J'(K)}{B'(K) + E'(K)} \right| \cdot \left| \ker\left(H^1(K, B') \rightarrow H^1(K, J')\right) \right|$$

depends on the choice of T in Section 1. There are two interesting choices of T, which are the two extreme cases.

The first is where T consists of conjugacy classes of *all* newforms of level dividing N that have analytic rank more than one. Then by Proposition 1.3, the product above is allowed to be divisible by all primes p such that f is congruent to an eigenform g of analytic rank bigger than one modulo some prime ideal over p; such eigenforms g are precisely all of the eigenforms on $\Gamma_0(N)$ using which the theory of visibility can be used to construct non-trivial elements of the the Shafarevich-Tate group of E as in Theorem 1.4. Thus in some sense, we are getting the most out of the theorem with this choice of T.

The other extreme choice of T is that it consists of the conjugacy class of a *single* newform on $\Gamma_0(N)$ that has analytic rank more than one. The advantage of this choice is that we are able to prove a sort of converse to Proposition 1.3:

Proposition 2.1. *Recall that f is a newform with integer Fourier coefficients that has analytic rank one. Suppose there is a newform g with integral Fourier coefficients that has analytic rank greater than one such that f and g are congruent modulo an odd prime q. Take T to be the singleton set $\{g\}$ in the definition of J' and B' in Section 1. Suppose that $q^2 \nmid N$, $A_f^\vee[q]$ and $A_g^\vee[q]$ are irreducible representations of the absolute Galois group of $\mathbf{Q}$, and q does not divide the order of the torsion subgroup of the projection of $\mathbf{T}P$ in J'. Then q divides the product*

$$\left| \frac{J'(K)}{B'(K) + E'(K)} \right| \cdot \left| \ker\left(H^1(K, B') \rightarrow H^1(K, J')\right) \right|.$$

Proof. The proposition essentially follows from the main result of [Aga08], as we now indicate. Take $E = A_f^\vee$ and $F = A_g^\vee$ in loc. cit. Then since B'

is isogenous to $A_g^\vee$, we see that $F' = B'$ in the notation of loc. cit. Let r denote the highest power of q modulo which f and g are congruent. Then condition (a) on r in Theorem 1.4 of loc. cit. is satisfied. By the discussion just before Lemma 1.2 of loc. cit., the hypotheses that q is odd, $q^2 \nmid N$, and $A_f^\vee[q]$ and $A_g^\vee[q]$ are irreducible imply that r satisfies condition (b) in Theorem 1.4 of loc. cit. The hypothesis that q does not divide the order of the torsion subgroup of the projection of $\mathbf{T}P$ in J' implies that condition (c) in Theorem 1.4 of loc. cit. is satisfied. Then the proof of Theorem 1.4 of loc. cit. shows that r divides

$$\left| \frac{J'(K)}{B'(K) + E'(K)} \right| \cdot \left| \ker\big(H^1(K, B') \to H^1(K, J') \big) \right|$$

(the statement just after Lemma 2.1 of loc. cit. shows that r/r' divides the first factor in the product above, and the very last statement shows that r' divides the second factor in the product above, where r' is a certain divisor of r defined in loc. cit.). The proposition now follows. $\square$

As mentioned before, the proposition above is a result that is in a direction opposite to that of Proposition 1.3, and is a partial result in trying to characterize the primes that divide the factor

$$\left| \frac{J'(K)}{B'(K) + E'(K)} \right| \cdot \left| \ker\big(H^1(K, B') \to H^1(K, J') \big) \right|$$

of the "analytic" left side of the Birch and Swinnerton-Dyer conjectural formula (1), which we related to the "arithmetic" right side of this formula. Notice the similarity with the rank zero case in [Aga07], where we isolated a factor of the "analytic" left side of the Birch and Swinnerton-Dyer formula that could be characterized in terms of congruences analogous to the ones above and related these congruences to the "arithmetic" right side (the results for the analytic rank zero case are more precise).

Remark 2.2. One question that remains is whether the product

$$\left| \frac{J'(K)}{B'(K) + E'(K)} \right| \cdot \left| \ker\big(H^1(K, B') \to H^1(K, J') \big) \right|$$

is non-trivial in general, and if so, how often. It would be nice to have some numerical data where the hypotheses of Proposition 2.1 are satisfied, so that the product above is non-trivial. If this happens, then in view of Theorem 1.4, we expect that either $Ш(E)$ is non-trivial or an arithmetic component group of E is non-trivial, of which the former seems more likely.

Since it is difficult to compute the actual order of the Shafarevich-Tate group, we looked at the Birch and Swinnerton-Dyer conjectural orders in Cremona's online "Elliptic curve data" [Cre]. Unfortunately the conjectural orders of the Shafarevich-Tate groups of elliptic curves of analytic rank one at low levels are usually one or powers of 2, which makes it difficult to find examples where the hypotheses of Proposition 2.1 can be verified easily. For levels up to 30000, we found only one optimal elliptic curve of Mordell-Weil rank one for which the conjectural order of the Shafarevich-Tate group was divisible by an *odd* prime: the curve E with label 28042A, for which the conjectural order of the Shafarevich-Tate group is 9. At the same level, the curve $F = 28042B$ has Mordell-Weil rank 3 and the newforms f and g corresponding to 28042A and 28042B respectively have Fourier coefficients that are congruent modulo 3 for every prime index up to 100 (although this is not enough to conclude that the newforms are congruent modulo 3 for all Fourier coefficients, cf. [AS02a]). We do not know how to verify the hypotheses in Proposition 2.1 that 3 does not divide the order of the torsion subgroup of the projection of $\mathbf{T}P$ in J' and that $E[3]$ and $F[3]$ are irreducible representations of the Galois group of K (we remark though that by [Cre], E and F have no 3-torsion over $\mathbf{Q}$). So while we cannot be sure that Proposition 2.1 applies to show that 3 divides the product

$$\left|\frac{J'(K)}{B'(K) + E'(K)}\right| \cdot \left|\ker\left(H^1(K, B') \to H^1(K, J')\right)\right|,$$

it is quite encouraging that for the first example where the conjectural order of the Shafarevich-Tate group of an elliptic curve is divisible by an odd prime, there is a congruence modulo the same prime that might show that the product above is divisible by the prime in question, and hence explain why the prime divides the order of the Shafarevich-Tate group.

Remark 2.3. Let q be a prime that does not divide the order of the torsion subgroup of $\pi''(\mathbf{T}P)$. Recall the conjectural equation (4), which is predicted by the Birch and Swinnerton-Dyer conjecture, and which we repeat below:

$$\left|c_{A_f} \cdot \prod_{p|N} c_p(E)\right|_q \cdot \sqrt{|\text{Ш}(E/K)|_q}$$

$$\stackrel{?}{=} \left|\frac{J'(K)}{B'(K) + E'(K)}\right|_q \cdot \left|\ker\left(H^1(K, B') \to H^1(K, J')\right)\right|_q \cdot \left|\frac{B'(K) + E'(K)}{B'(K) + \pi''(\mathbf{T}P)}\right|_q.$$

While we were able to relate certain primes dividing the product

$$\left|\frac{J'(K)}{B'(K) + E'(K)}\right|_q \cdot \left|\ker\left(H^1(K, B') \to H^1(K, J')\right)\right|_q$$

9

on the right side of the equation above to its left side, one question that remains is to interpret the remaining factor

$$\left| \frac{B'(K) + E'(K)}{B'(K) + \pi''(\mathbf{T}P)} \right|_q$$

on the right side of equation, which is expected to divide the left side of equation above. Now we were able to relate the primes dividing the product

$$\left| \frac{J'(K)}{B'(K) + E'(K)} \right| \cdot \left| \ker\left(H^1(K, B') \to H^1(K, J')\right) \right|$$

to $\prod_{p|N} c_p(E) \cdot \sqrt{|\text{Ш}(E/K)|}$ in Theorem 1.4 using the theory of visibility and the existence of congruences modulo prime ideals over q with eigenforms at the *same* level N that have analytic rank more than one. If M is a positive integer, then f can be mapped to $S_2(\Gamma_0(NM), \mathbf{C})$ using suitable degeneracy maps, and if there is an eigenform at the *higher* level NM that is congruent to the image of f in $S_2(\Gamma_0(NM), \mathbf{C})$ modulo some prime ideal over a prime q, then again the theory of visibility can sometimes be used to show that q divides the order of $\text{Ш}(E)$ (e.g., see [AS02b, §4.2]). We loosely call this phenomenon "visibility at higher level". It has been conjectured that any element the Shafarevich-Tate group can be explained by visibility at some higher level (see Conjecture 7.1.1 in [JS07] for details and a precise statement). Thus we suspect that one may be able to explain the factor

$$\left| \frac{B'(K) + E'(K)}{B'(K) + \pi''(\mathbf{T}P)} \right|_q$$

using the idea of visibility at higher level, at least in specific examples. The situation is similar to the case where f has analytic rank one [Aga07], when we were able to understand a certain factor using the theory of visibility and congruences of f with eigenforms of higher rank on $\Gamma_0(N)$, and suspected that to explain the remaining factor, one would need to use visibility at a higher level.

In view of Remarks 2.2 and 2.3, we hope that our article motivates more detailed computations similar to those in [AS05] for the analytic rank one case, especially since all this pertains to the Birch and Swinnerton-Dyer conjecture.

3 Proof of Proposition 1.3

Following a similar situation in [CM00], consider the short exact sequence

$$0 \to B' \cap E' \to B' \oplus E' \to J' \to 0, \tag{5}$$

where the map $B' \cap E' \to B' \oplus E'$ is the anti-diagonal embedding $x \mapsto (-x, x)$ and the map $B' \oplus E' \to J'$ is given by $(b', e') \mapsto b' + e'$.

Lemma 3.1. *Suppose q is a prime that divides*

$$\left| \frac{J'(K)}{B'(K) + E'(K)} \right|.$$

Then q divides the order of $B' \cap E'$.

Proof. The long exact sequence associated to (5) gives us

$$\cdots \to B'(K) \oplus E'(K) \to J'(K) \to H^1(K, B' \cap E') \to H^1(K, B' \oplus E') \to \cdots ,$$

from which we get

$$\frac{J'(K)}{B'(K) + E'(K)} = \ker \left(H^1(K, B' \cap E') \to H^1(K, B' \oplus E') \right). \tag{6}$$

Since q divides $\left| \frac{J'(K)}{B'(K)+E'(K)} \right|$, there is an element σ of the right hand side of (6) of order q. Since $B' \cap E'$ is finite, so is $H^1(K, B' \cap E')$, and its order divides $|B' \cap E'|$. Hence q divides $|B' \cap E'|$. $\square$

Lemma 3.2. *Suppose q is a prime that divides $\left| \ker \left(H^1(K, B') \to H^1(K, J') \right) \right|$. Then q divides the order of $B' \cap E'$.*

Proof. By hypothesis, there is an element σ of $\ker \left(H^1(K, B') \to H^1(K, J') \right)$ of order q. The long exact sequence associated to (5) gives us

$$\cdots \to H^1(K, B' \cap E') \to H^1(K, B') \oplus H^1(K, E') \to H^1(K, J') \to \cdots . \tag{7}$$

The element $(\sigma, 0) \in H^1(K, B') \oplus H^1(K, E')$ of order q in the middle group in (7) maps to zero in the rightmost group $H^1(K, J')$ in (7), and thus by the exactness of (7), there is a non-trivial element $\sigma' \in H^1(K, B' \cap E')$ of order divisible by q that maps to $(0, \sigma) \in H^1(K, B') \oplus H^1(K, E')$. Again, since $B' \cap E'$ is finite, so is $H^1(K, B' \cap E')$, and its order divides $|B' \cap E'|$. Hence q divides $|B' \cap E'|$. $\square$

11

Proof of Proposition 1.3. By Lemmas 3.1 and 3.2, we see that q divides the order of $B' \cap E'$, which proves the first claim in Proposition 1.3. The second claim follows from the first, using an argument similar to the one in [Aga07, §5], which in turn mimics the proof that the modular degree divides the congruence number [ARS07], as we now explain.

If h is a newform of level N_h dividing N, then let B_h denote the abelian subvariety of $J_0(N_h)$ associated to h by Shimura [Shi94, Thm. 7.14], and let J_h denote the sum of the images of B_h in $J = J_0(N)$ under the usual degeneracy maps; note that J_h depends only on the Galois conjugacy class of h. Let C denote $(I_f \cap I_T)J$. Then C is the abelian subvariety of J generated by J_g where g ranges over Galois conjugacy classes of newforms of level dividing N other than orbit of f and other than the classes in T. Let B denote abelian subvariety of J generated by J_g where g ranges over Galois conjugacy classes of newforms of level dividing N other than the orbit of f and let A denote abelian subvariety of J generated by J_g where g ranges over Galois conjugacy classes of newforms of level dividing N other than the classes in T. Then $E' = A/C$ and $B' = B/C$. Now applying the arguments of [Aga07, §5] but with A, B, and C as above, the fact that q divides the order of $E' \cap B' = A/C \cap B/C$ implies that there is an eigenform g in the subspace of $S_2(\Gamma_0(N), \mathbf{C})$ generated by the newforms in T such that f is congruent to g modulo a prime ideal $\mathfrak{q}$ over q in the ring of integers of the number field generated by the Fourier coefficients of f and g. The second claim in Proposition 1.3 follows, considering that every newform g in T has analytic rank more than one. $\square$

References

[Aga07] A. Agashe, *A visible factor of the special L-value*, submitted (2007), available at arXiv:0810.2477 or
http://www.math.fsu.edu/$\sim$ agashe/math.html.

[Aga08] _____, *Visibility and the Birch and Swinnerton-Dyer conjecture for analytic rank one*, submitted (2008), available at arXiv:0810.2487 or
http://www.math.fsu.edu/$\sim$agashe/math.html.

[ARS07] A. Agashe, K. Ribet, and W. A. Stein, *The modular degree, congruence primes, and multiplicity one*, submitted (2007), available at
http://www.math.fsu.edu/$\sim$agashe/moddeg3.html.

[AS02a]   A. Agashe and W. A. Stein, Appendix to Joan-C. Lario and René Schoof, *Some computations with Hecke rings and deformation rings*, Experiment. Math. **11** (2002), no. 2, 303–311.

[AS02b]   Amod Agashe and William Stein, *Visibility of Shafarevich-Tate groups of abelian varieties*, J. Number Theory **97** (2002), no. 1, 171–185.

[AS05]   _____, *Visible evidence for the Birch and Swinnerton-Dyer conjecture for modular abelian varieties of analytic rank zero*, Math. Comp. **74** (2005), no. 249, 455–484 (electronic), With an appendix by J. Cremona and B. Mazur.

[CM00]   J. E. Cremona and B. Mazur, *Visualizing elements in the Shafarevich-Tate group*, Experiment. Math. **9** (2000), no. 1, 13–28. MR 1 758 797

[Cre]   J. E. Cremona, *Elliptic curve data*, http://www.warwick.ac.uk/∼masgaj/ftp/data/index.html.

[DSW03]   Neil Dummigan, William Stein, and Mark Watkins, *Constructing elements in Shafarevich-Tate groups of modular motives*, Number theory and algebraic geometry, London Math. Soc. Lecture Note Ser., vol. 303, Cambridge Univ. Press, Cambridge, 2003, pp. 91–118. MR MR2053457

[Gro91]   B. H. Gross, *Kolyvagin's work on modular elliptic curves*, L-functions and arithmetic (Durham, 1989), Cambridge Univ. Press, Cambridge, 1991, pp. 235–256.

[GZ86]   B. Gross and D. Zagier, *Heegner points and derivatives of L-series*, Invent. Math. **84** (1986), no. 2, 225–320. MR 87j:11057

[JS07]   Dimitar P. Jetchev and William A. Stein, *Visibility of the Shafarevich-Tate group at higher level*, Doc. Math. **12** (2007), 673–696.

[KL89]   V. A. Kolyvagin and D. Y. Logachev, *Finiteness of the Shafarevich-Tate group and the group of rational points for some modular abelian varieties*, Algebra i Analiz **1** (1989), no. 5, 171–196.

[Kol90] V. A. Kolyvagin, *Euler systems*, The Grothendieck Festschrift, Vol. II, Progr. Math., vol. 87, Birkhäuser Boston, Boston, MA, 1990, pp. 435–483.

[McC91] W. G. McCallum, *Kolyvagin's work on Shafarevich-Tate groups*, L-functions and arithmetic (Durham, 1989), Cambridge Univ. Press, Cambridge, 1991, pp. 295–316. MR 92m:11062

[Shi94] G. Shimura, *Introduction to the arithmetic theory of automorphic functions*, Princeton University Press, Princeton, NJ, 1994, Reprint of the 1971 original, Kan Memorial Lectures, 1.